How to configure TMG features on Fortigate

…a small guide to find the right switches

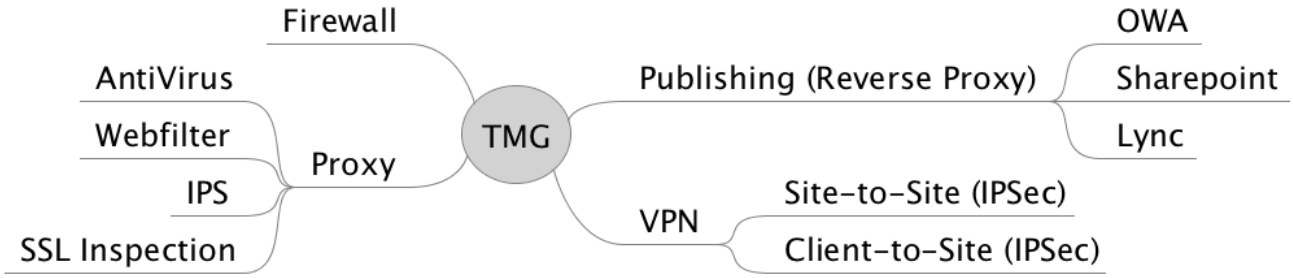
Version 0.1
Date: 24. June 2013
FortiOS Release: 5.0.3

How to configure TMG features on Fortigate

1. Introduction

This document is intended as a resource for technical experienced readers and Fortigate Guru's. It tries to give an explanation of the features used and shows a way to use them. Some chapters will show a high amount of links to other resources while others use explicit samples.
As there is usually more than one way to succeed, this document doesn't claim to be the complete guide, instead it's intention is to give the reader an idea how TMG's features can be mapped to FortiGate.

This diagram points out the most requested features, which will be covered in this document.



For an environment with specialized requirements, Fortinet offers other products that might offer more flexibility or granularity than FortiGate.

- Web Application Firewall (FortiWeb),
- Mail Security (FortiMail),
- Loadbalancer (FortiBalancer).

An interesting aspect of Fortinet products is the simple license model. Specifically the FortiGate is not licensed on features or functions. All features[1] are available without additional costs. Therefore the selection of the right model is mainly based on throughput. Additional services like hardware and software support, as well as definition updates for AntiVirus, IPS, Urlfilter, etc. can be added when required.

A list of authorized partners and distributors is available here:
http://www.fortinet.com/partners/emeapartners.html

Further information can be found on the following Fortinet websites:

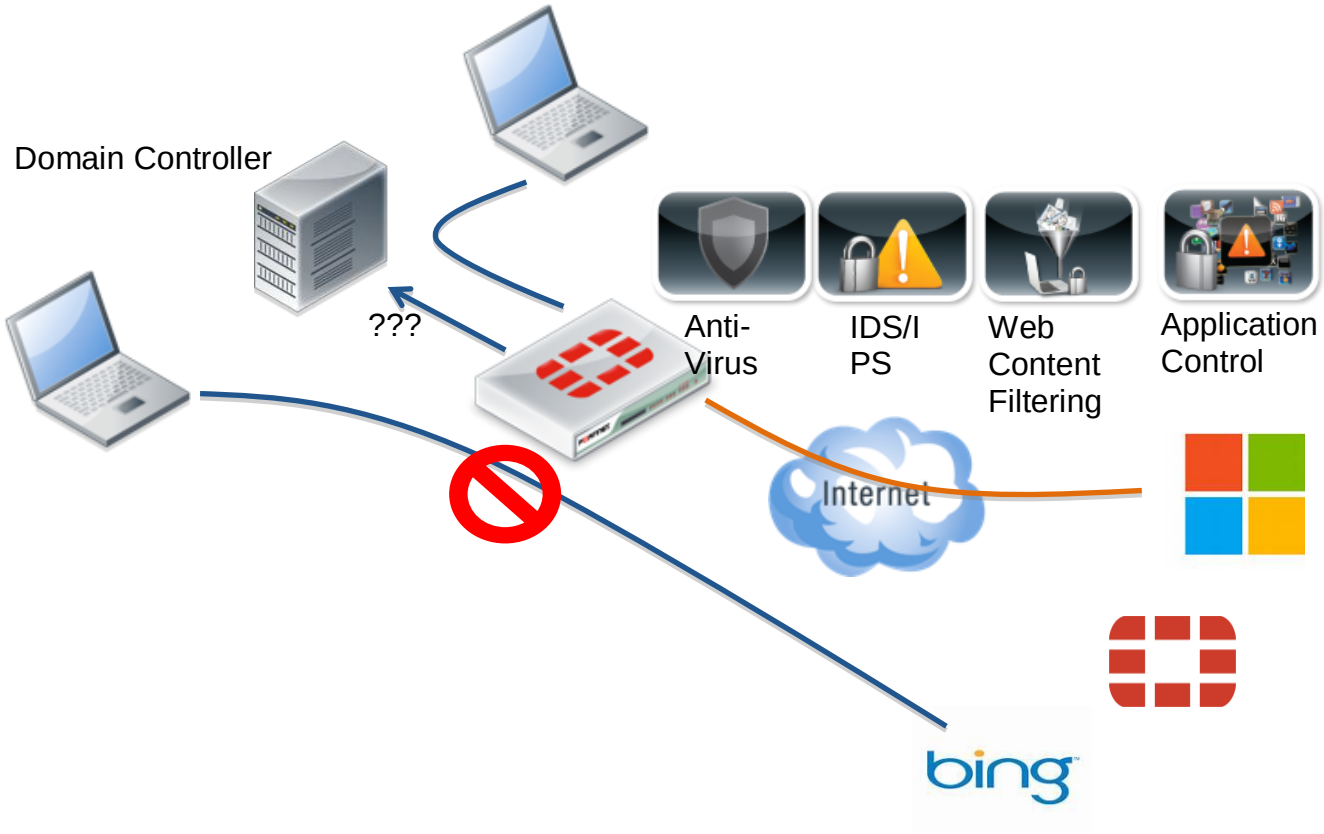
http://www.fortinet.com
http://docs.fortinet.com
http://kb.fortinet.com
http://www.fortinet.com/partners/partner_program/fppemea.html

[1] Due to technical capabilities, the models FortiGate-90D and below offer a limited feature set.

2. TMG features
    a. Proxy

Feature Description

One of the oldest and most used functions of TMG was the role as a proxy server to enable Internet access for clients. In this context a key aspect was that users did not have to sign-in a second time.
Such a Single-Sign-On (SSO) feature is part of the FortiGate feature set and fully integrated. Thereby the FortiGate communicates with the Active Directory domain controllers and is able to read and evaluate the rights and permissions of users signed-in.
Additionally comprehensive security functions like AntiVirus, Intrusion Prevention, Web Filter and Application Control can be used.



Nowadays almost every application tries to communicate via HTTP or HTTPS with various servers on the Internet. With application control enabled the IP traffic and packets are inspected in detail. Thus FortiGate allows for detecting and differentiating between various applications, e.g. Skype, Skydrive, WindowsUpdate, NetMeeting and many more. Of course detection is not limited to a certain vendor. Many different applications are recognized as well as either dangerous or potentially harmful programs like botnet activity, remote access or file sharing applications.

The latest list of applications is available at http://www.fortiguard.com

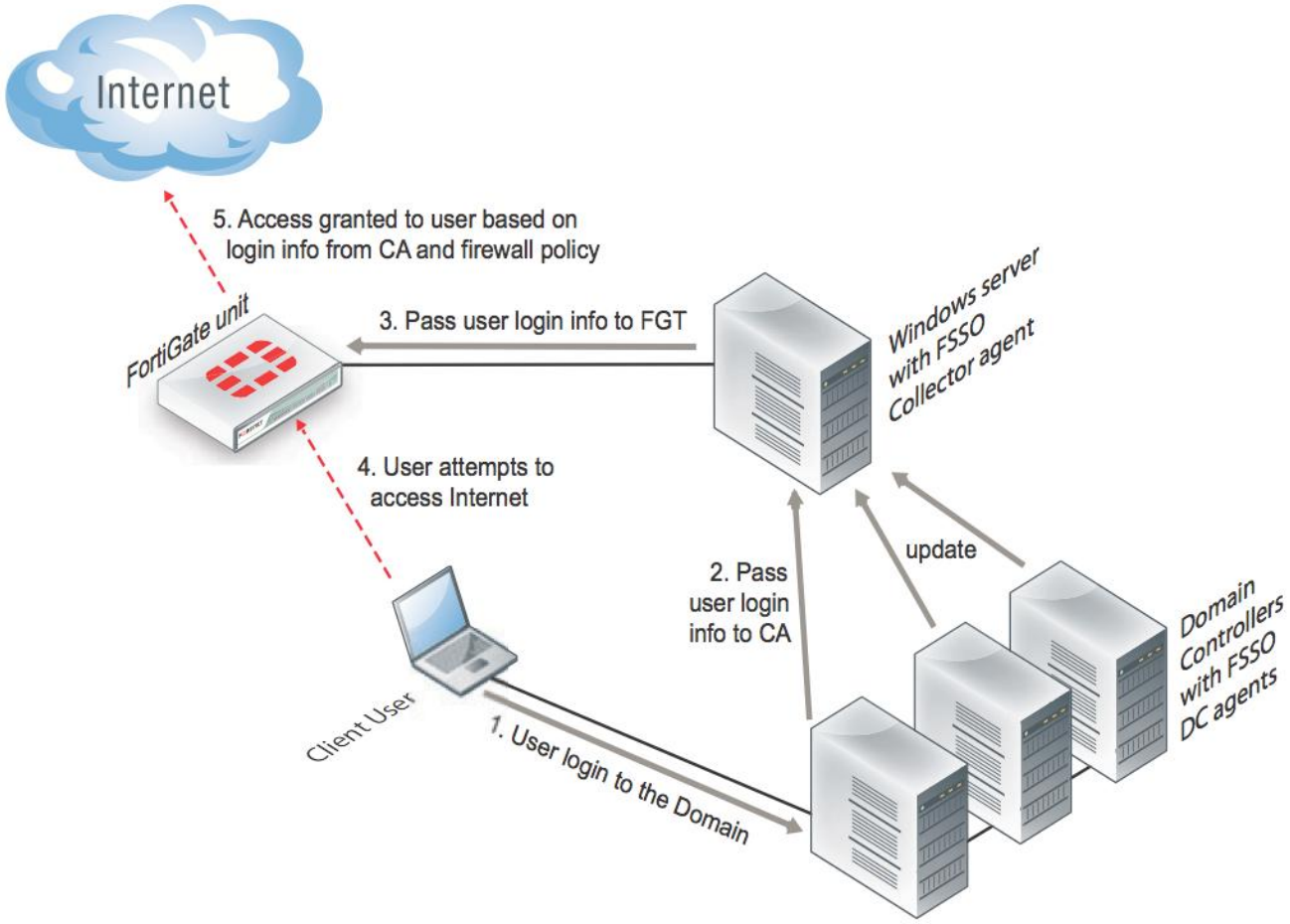
Implementing it

The proxy feature can be split in two parts
- authentication
- content security

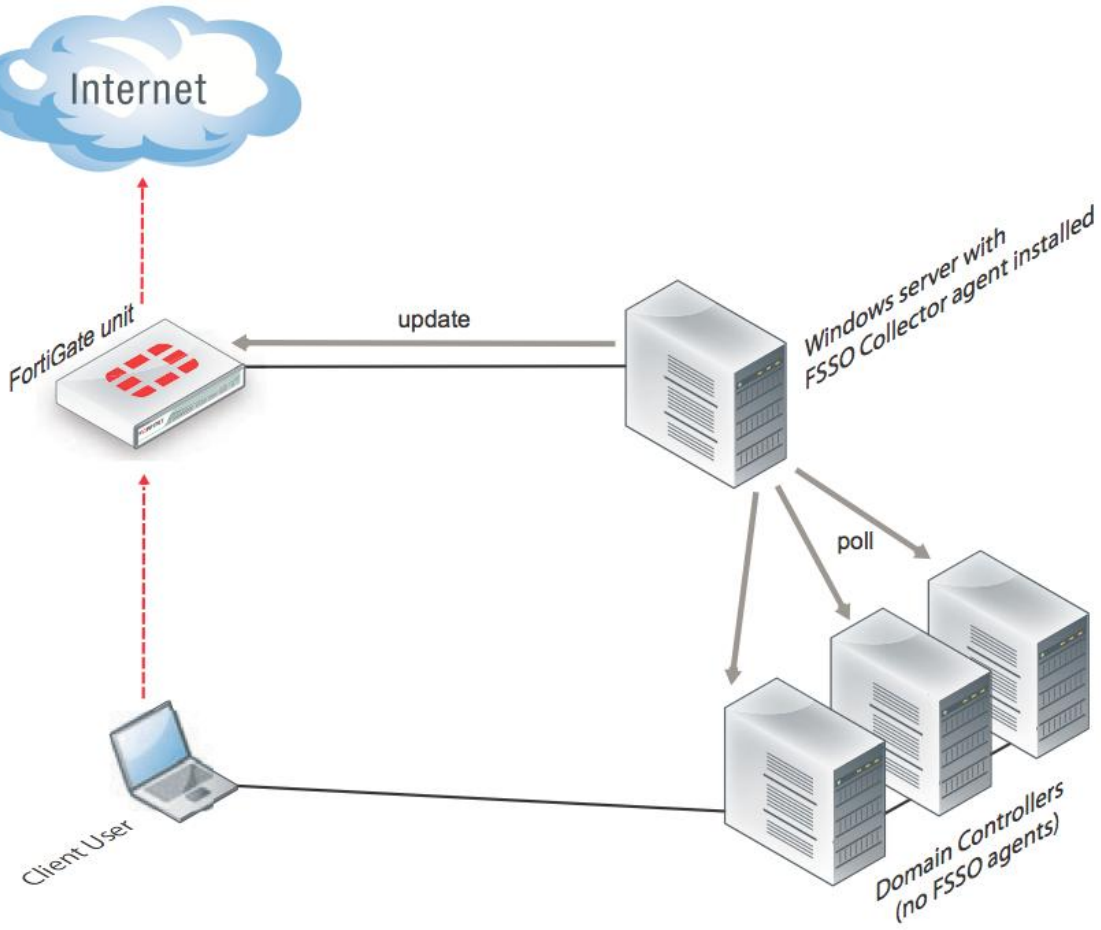
The authentication part can be done on Fortigate in various different ways.

1) Using DC Agent on Domain Controller
This method implies the installation of a software component on the domain controller, called "DC Agent".
The DC Agent doesn't communicate directly with FortiGate, it communicates with another software component "Collector Agent". The Collector Agent can be installed on a domain controller or on any Windows Server. The Collector Agent receives information from an arbitrary number of DC Agents and it can communicate this information to any FortiGate.

As the Collector Agent is a very critical component in the communication, it can be installed more than once for redundancy.

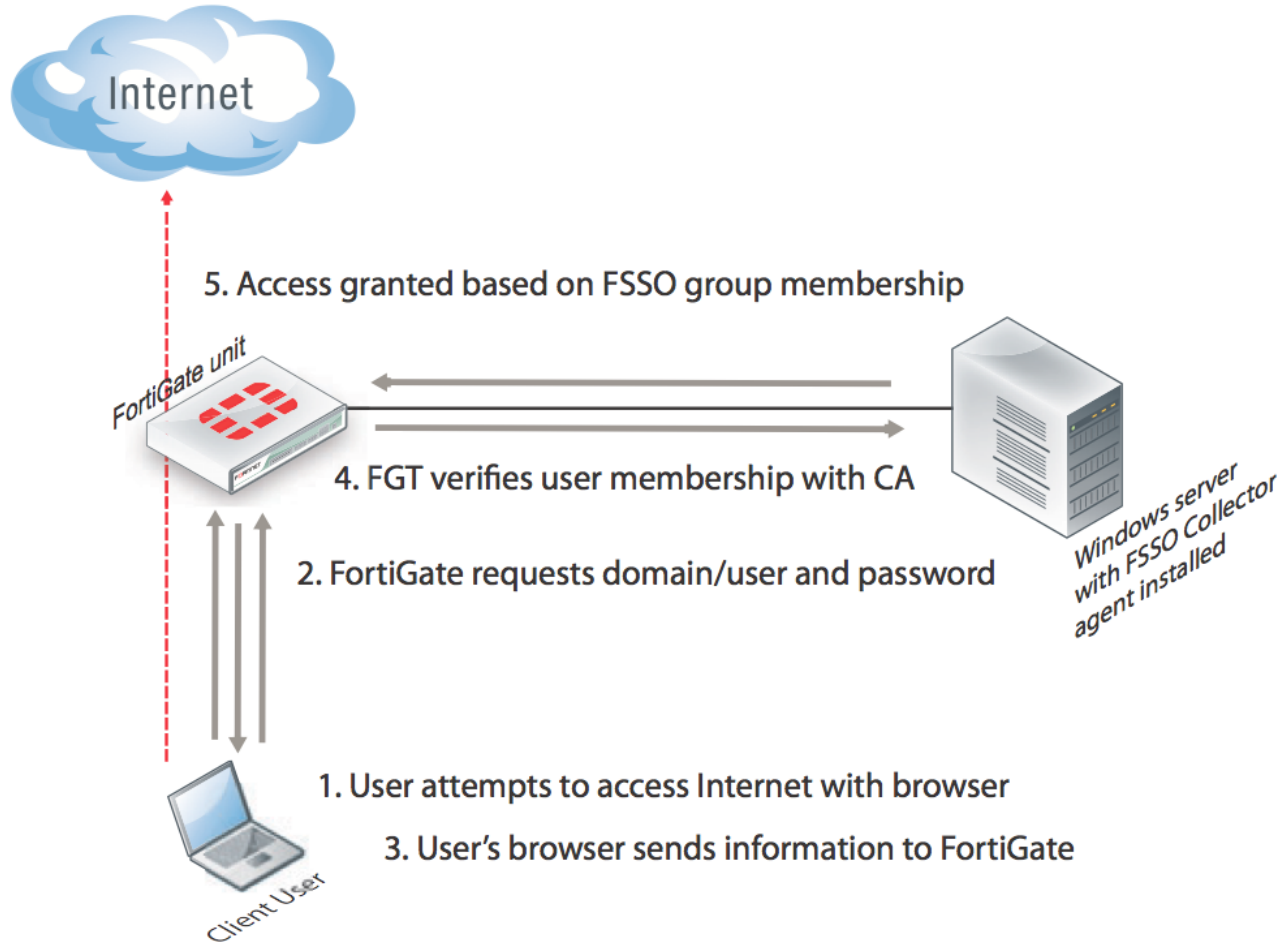


2) Polling from Collector Agent
Using this method, there is no need to install software on the domain controller. The Collector Agent will be installed on any Windows server and it will poll the domain controllers for their login events. This can be achieved by using Windows NetAPI or the Security Event log.

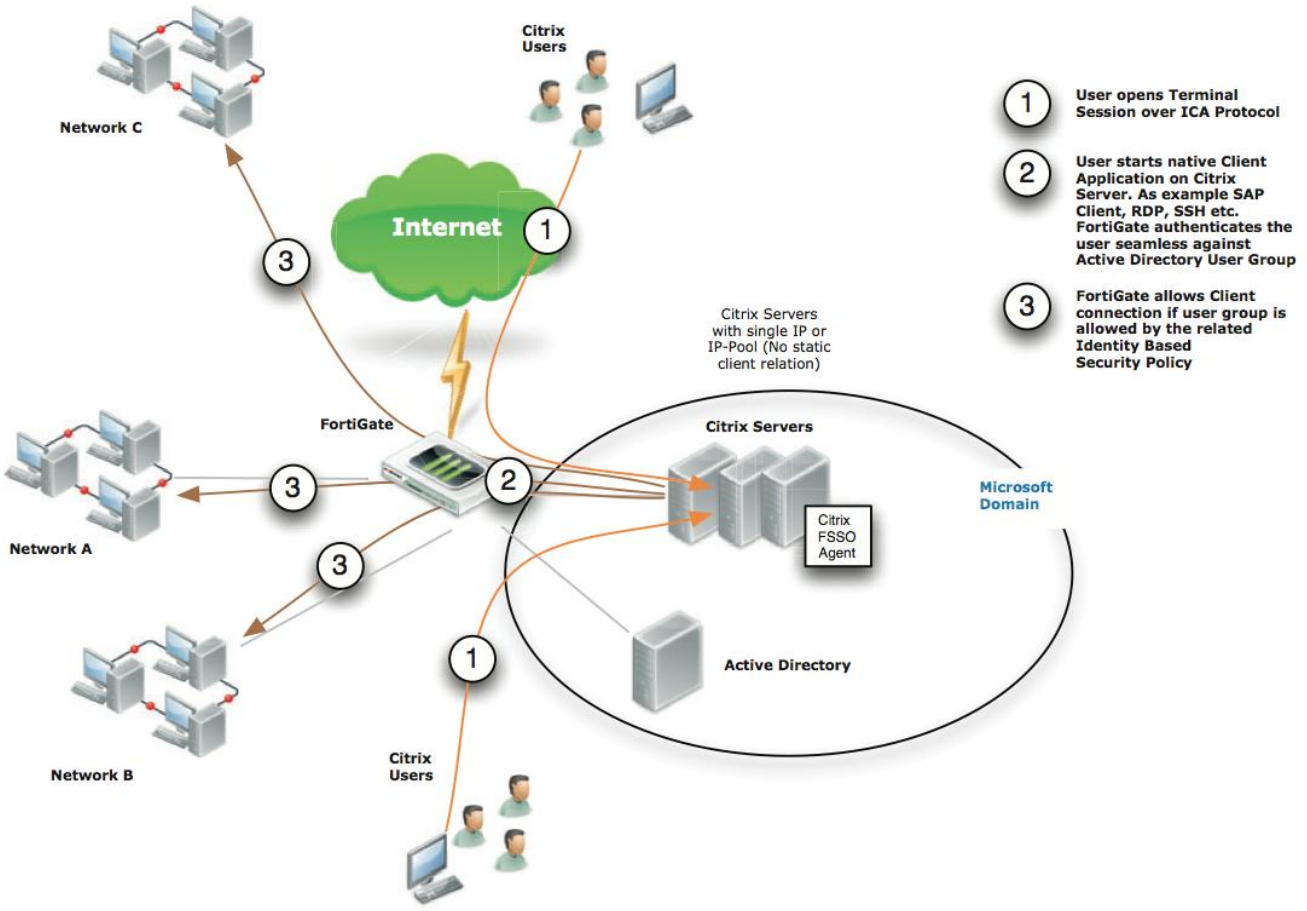


3) Polling directly from FortiGate
Starting with FortiOS 5, the polling mechanism from the Collector Agent has been implemented directly on FortiGate as well. FortiGate uses the Security Event log to get information about the logged on users from the domain controller.
This method is intended for small environment, where you don't have the resources to install Collector Agent on a server. Keep in mind that polling the servers increases the load on your FortiGate as well.

4) Authentication via NTLM
To utilize NTLM as source for authentication, FortiGate needs a Collector Agent to be installed in the network.



5) Terminal Servers
Terminal Servers have to be handled differently than user workstations. FSSO is intended to build a relationship between user and IP address. Users logged on to Microsoft or Citrix Terminal Servers typically don't have their own IP address; the address is shared among all users.
To overcome this limitation you need to install the TerminalServer Agent (TS Agent) on your server. This software component communicates again with the Collator Agent, telling the block of source ports that the terminal server has reserved for a specific user.



The installation and configuration of these components as well as additional information can be found in the “Authentication”/”Agent based FSSO” section of the FortiOS Handbook.
The FortiOS Handbook can be accessed on http://docs.fortinet.com in the according branch to your FortiOS version used.

The content security part is defined in the firewall policy. After having established the communication with the FSSO components, you can define a policy like this:

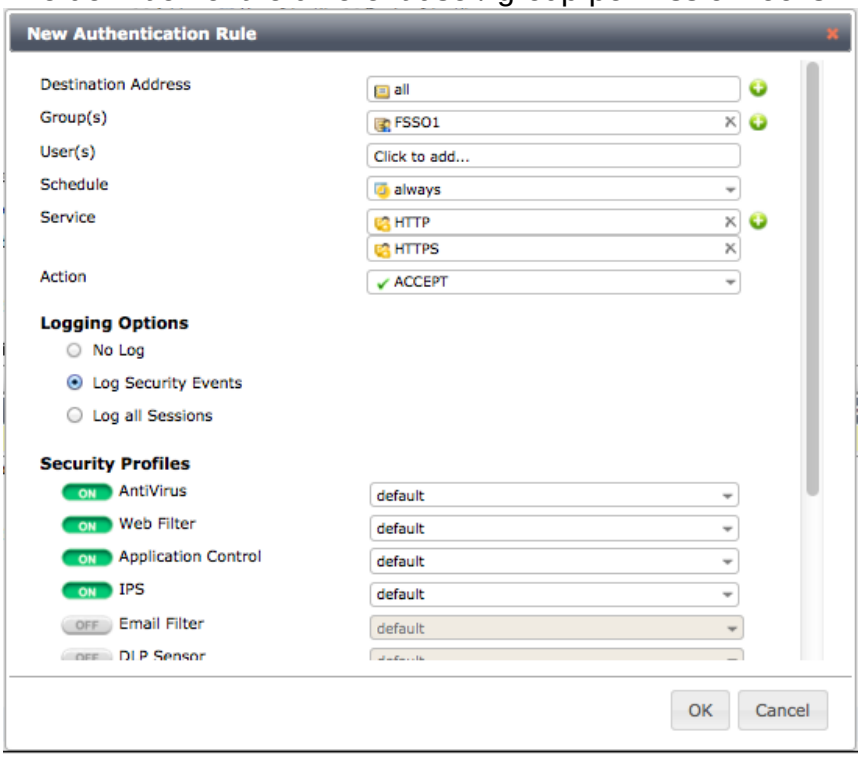
Policy Type: Firewall / VPN
Policy Subtype: Address / User Identity / Device Identity
Incoming Interface: internal
Source Address: net_1
Outgoing Interface: wan1 (Internet)
Enable NAT
Use Destination Interface Address — Fixed Port
Use Dynamic IP Pool — Click to add...
Use Central NAT Table
Enable Web cache
Enable WAN Optimization

Configure Authentication Rules

Create New | Edit | Delete

User/Group	Destination Address	Service	Schedule	Security	Traffic Shaping	Logging	Action
FSSO1	all	HTTP HTTPS	always				✓ ACCEPT
ANY	all	ALL	always	-			⊘ DENY

The definition of the different user/ group permission looks like this:



Having different groups with different security profiles gives you the power to control which user can access which resources in the network.

This is only a very quick overview about the transparent proxy implementation on FortiGate. It is only covered to give a reference about the configuration steps needed.

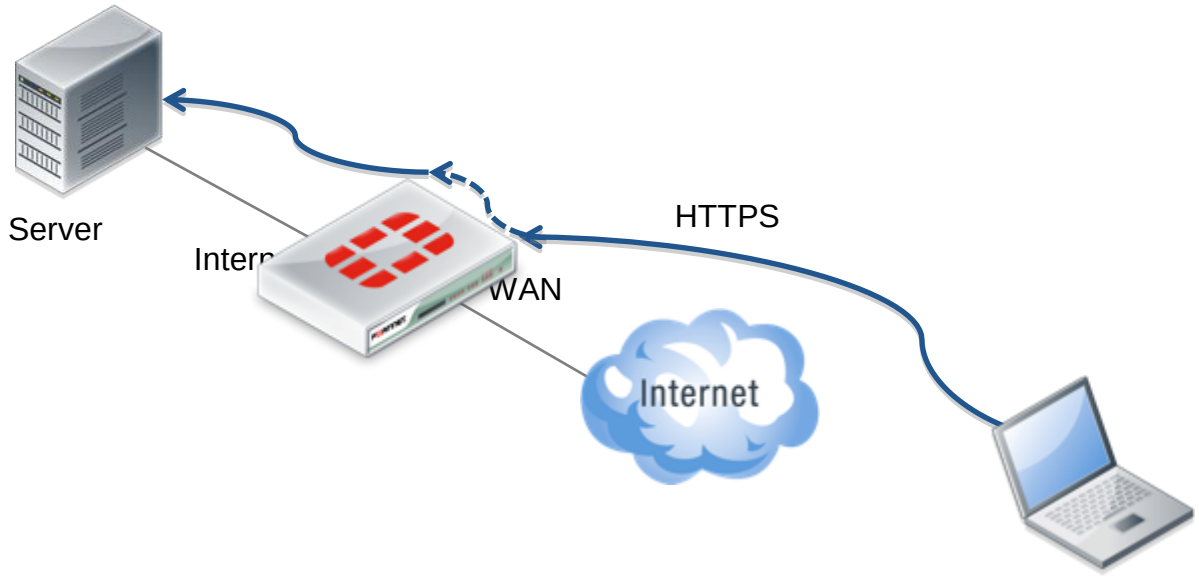
More details can be found in the FortiOS Handbook in the chapters Authentication, Firewalling and UTM.

b. OWA/SharePoint Publishing

Feature Description

From a functional perspective two things are important when it comes to publishing of Outlook Web Access or SharePoint services:

- Translation of the public IP address
- Exchanging the certificate, that external clients receive a valid, trusted and signed certificate.



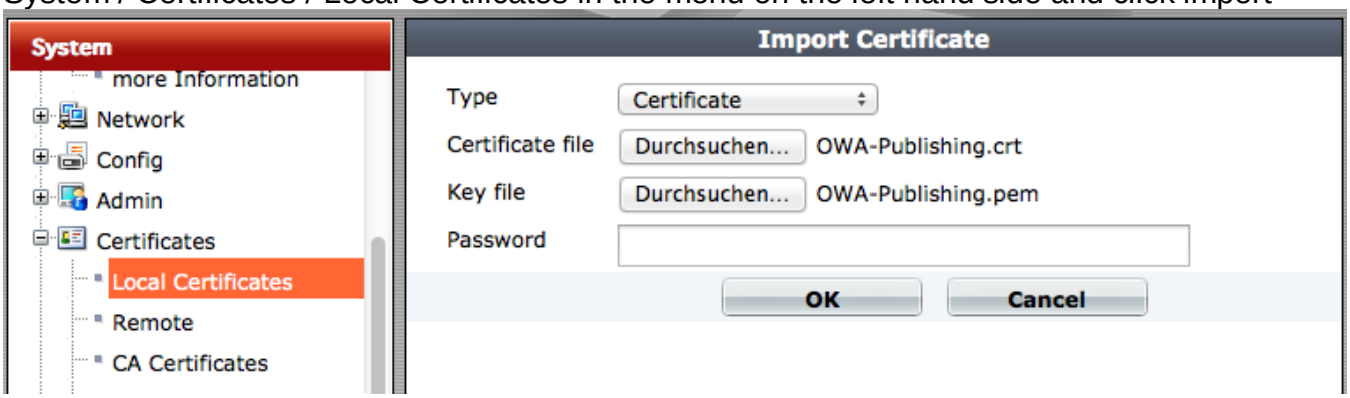
The following security features are a good extension, when it comes to securing the application:

- Scanning for attacks (Intrusion Prevention System)
- Scanning for viruses
- Checking of used paths for HTTP applications
- Checking on communications protocol in use (is it HTTP(S) or Activesync traffic/packets?)
- Blocking of IP address and/or alarm administrators when there are failed login attempts
- Load sharing when using multiple application servers

Implementing it

Certificate

The first step in configuring the publishing is importing a certificate. Select System / Certificates / Local Certificates in the menu on the left hand side and click import



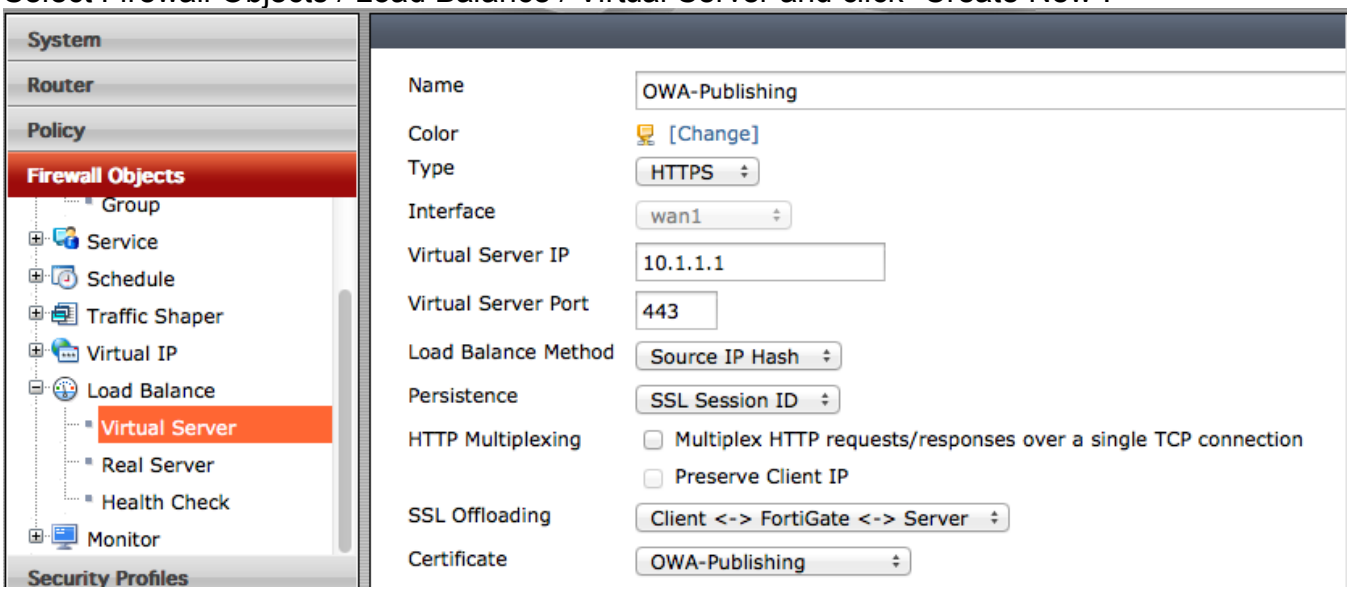
Select your certificate and key file and click “OK”.

Further information can be found in the documentation, accessible @ http://docs.fortinet.com

Knowledge Base article describing how to import certificates from IIS:
http://kb.fortinet.com/kb/microsites/search.do?cmd=displayKC&externalId=FD30129

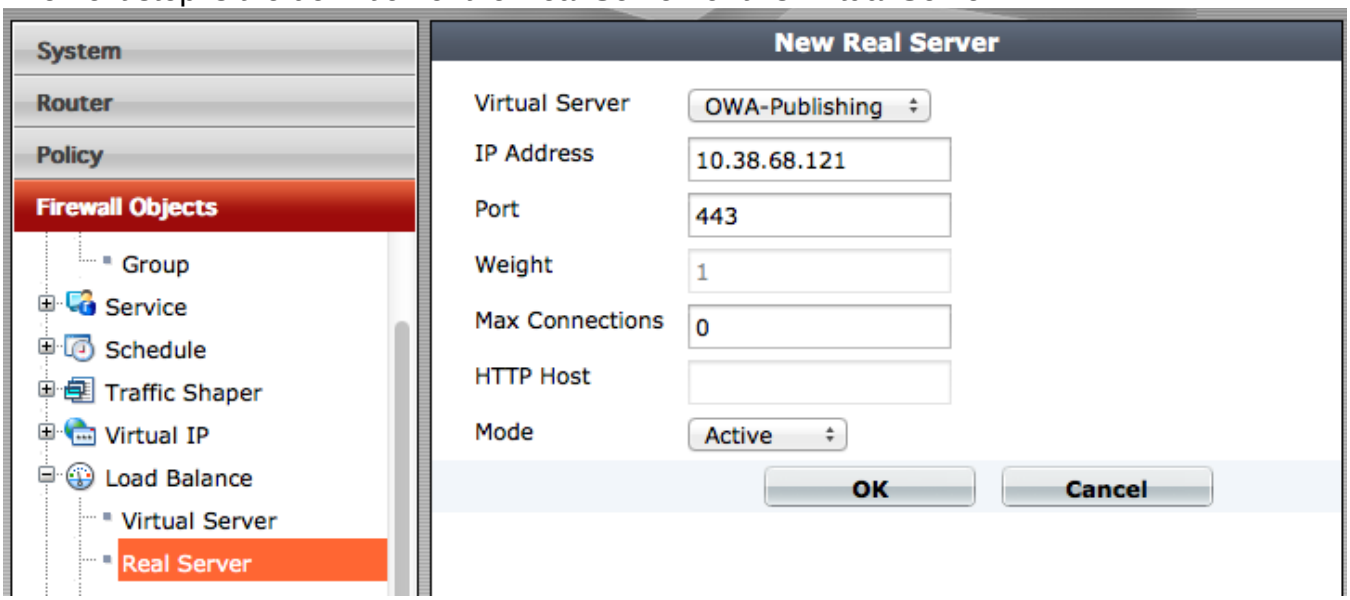
Load Balancer

To change the certificate and create a proxy behavior you have to configure a loadbancer. Select Firewall Objects / Load Balance / Virtual Server and click “Create New”.



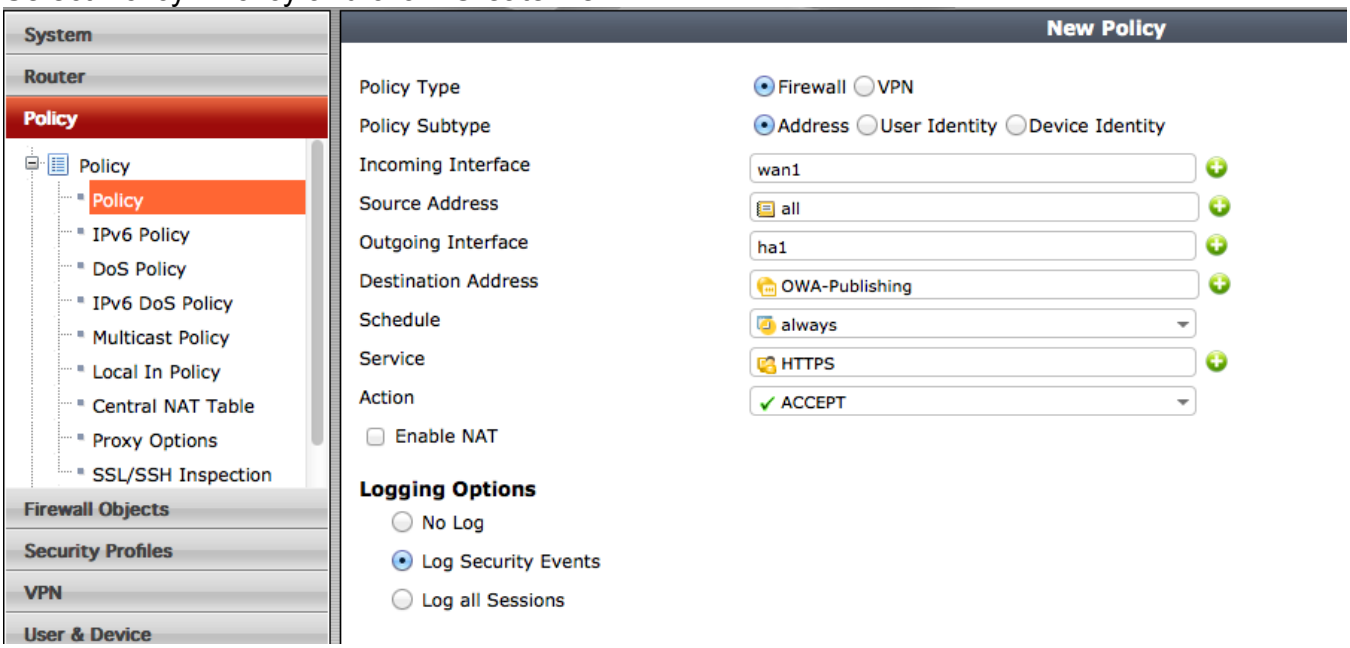
In this sample the Virtual Server IP has been assigned from the RFC1918 range. In a real life configuration you would choose one of your officially assigned IP addresses.

The next step is the definition of the Real Server for this Virtual Server:



Firewall Policy

The final step to enable traffic flow is the firewall policy.
Select Policy / Policy and click “Create New”



Select the interface where you connected you Internet access as “Incoming Interface” and “all” as “Source Address” to allow everybody on the Internet to access this service.
The “Outgoing Interface” reflects you interface on which the internal Server is accessible; the “Destination Address” is now the name of the Virtual Server you created in the previous step.
Limit the service to HTTPS as there is only HTTPS traffic to be forwarded.

With these steps you created the forwarding of the packets and the exchange of the SSL Server Certificate. Until now you do not have any additional security in place.

Adding security features

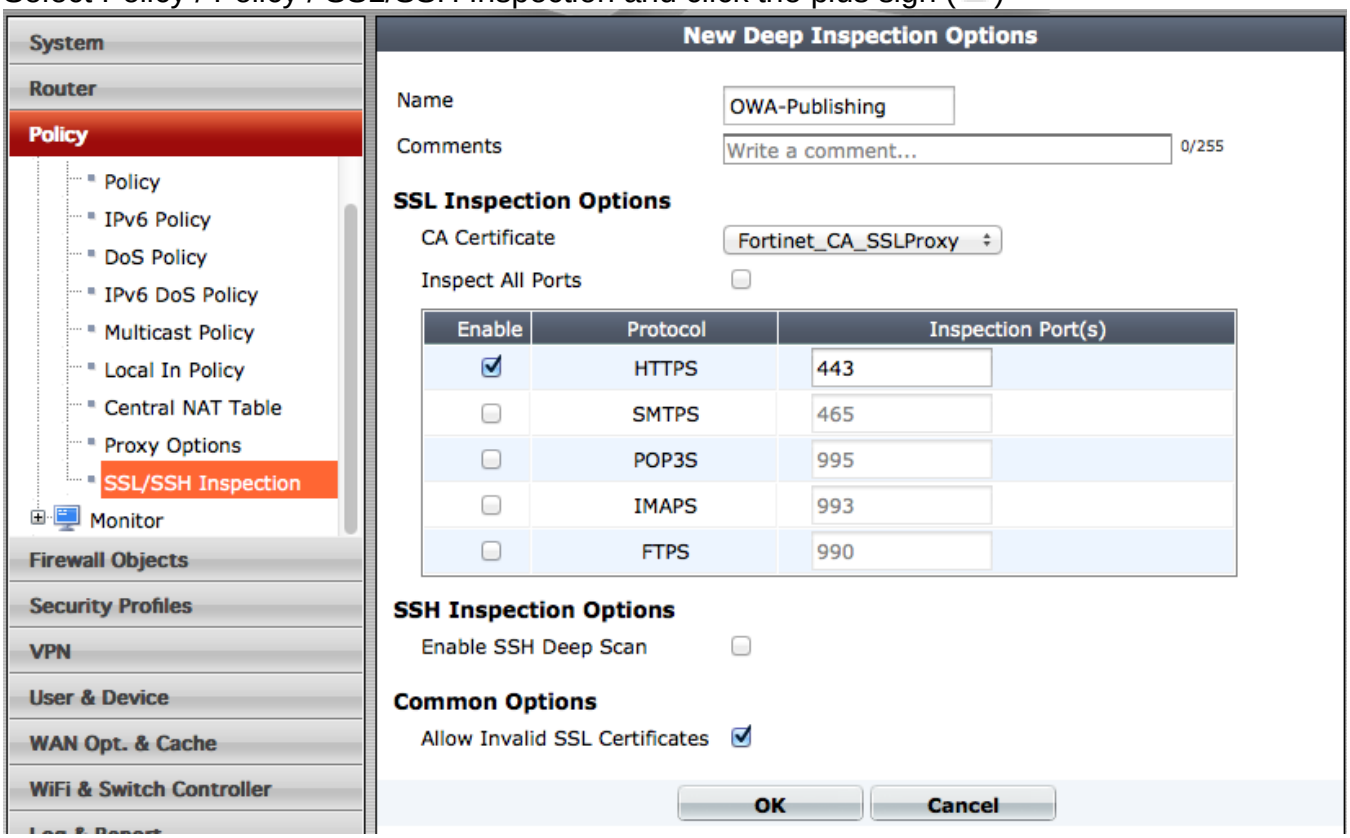
FortiGate offers a variety of security features. This guide covers the following

- Application Control
  Verifying that the application used is really the one we expect. Checking more than just destination TCP port
- IPS
- AntiVirus
- URL Filter

The inside FortiOS documents give a very good overview about the possibilities of these and other features. (http://docs.fortinet.com/ifos.html)
Detailed Information about all these features is available in the chapter “UTM” of “The FortiOS Handbook” (http://docs.fortinet.com/fgt50.html)

SSL Inspection

Prior to defining the content level security you have to define the SSL Inspection
Select Policy / Policy / SSL/SSH Inspection and click the plus sign ( )

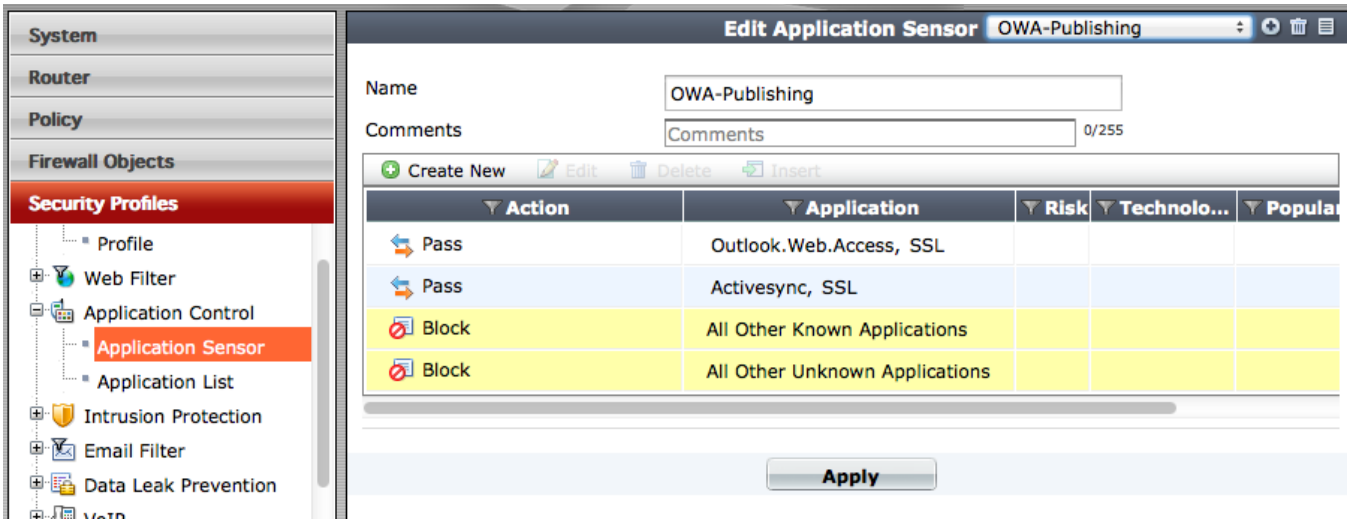


This enables your FortiGate to inspect the SSL encrypted traffic.
You can use the default CA certificate in this case as the encryption happens between the “backend” part of the reverse proxy of FortiGate and the server. Therefore the client will never see this certificate.
As the internal server might have a self signed certificated, enable “Allow invalid SSL Certificates”.

All these settings will only affect the traffic for the published application, and will not conflict with any other traffic inspection.

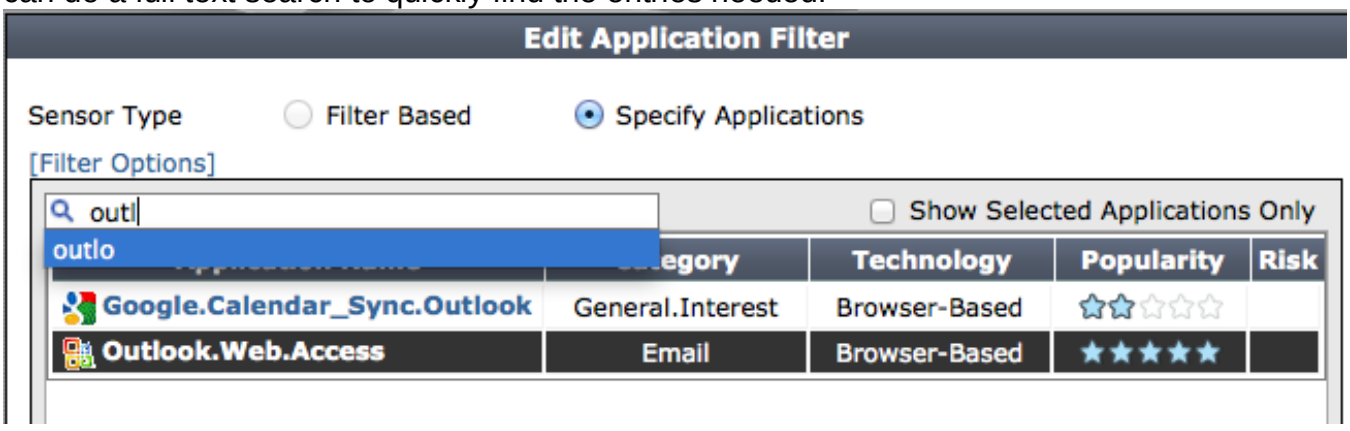
Application Control

First you have to create a new Application Sensor. Select Security Profiles / Application Control / Application Sensor and click the plus sign ( )



Note: Columns have been reordered to enlarge screenshot

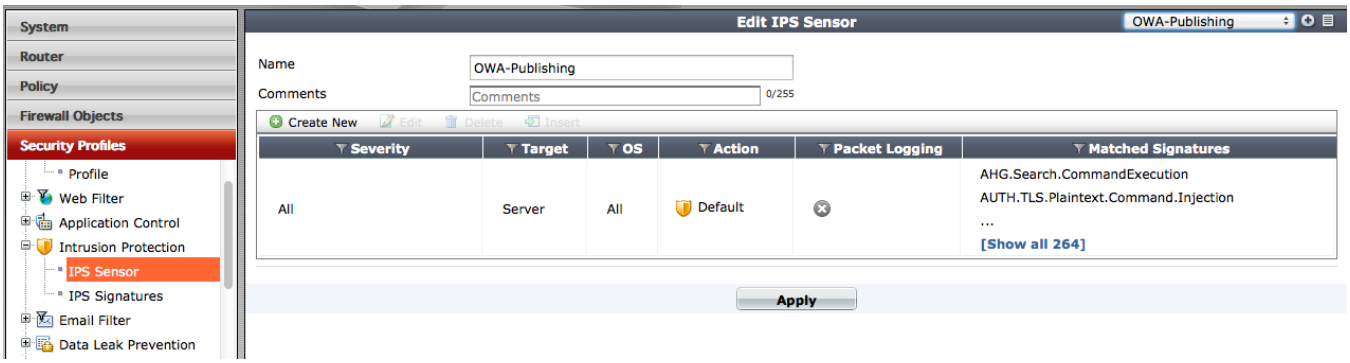
To select the applications you have to switch to Sensor Type “Specify Applications”, there you can do a full text search to quickly find the entries needed.



It is important to choose both the application and SSL in one “row” as the application traffic is both SSL and Outlook traffic at the same time.

IPS

To create a new Application Sensor select Security Profiles / Intrusion Protection / IPS Sensor and click the plus sign ( )



Within the GUI there is no possibility to create a filter based on the application. To achieve this you can use this CLI script, that can be pasted into a ssh console.

```
config ips sensor
    edit "OWA-Publishing"
            config entries
                edit 2
                    set application IIS MS_Exchange
                    set location server
                next
            end
    next
end
```

Note that the name used in the CLI lines correlates with the name in the screenshot. This setting activates any IPS signature for the Products Internet Information Server and Exchange. Future signatures will be activated automatically as well.

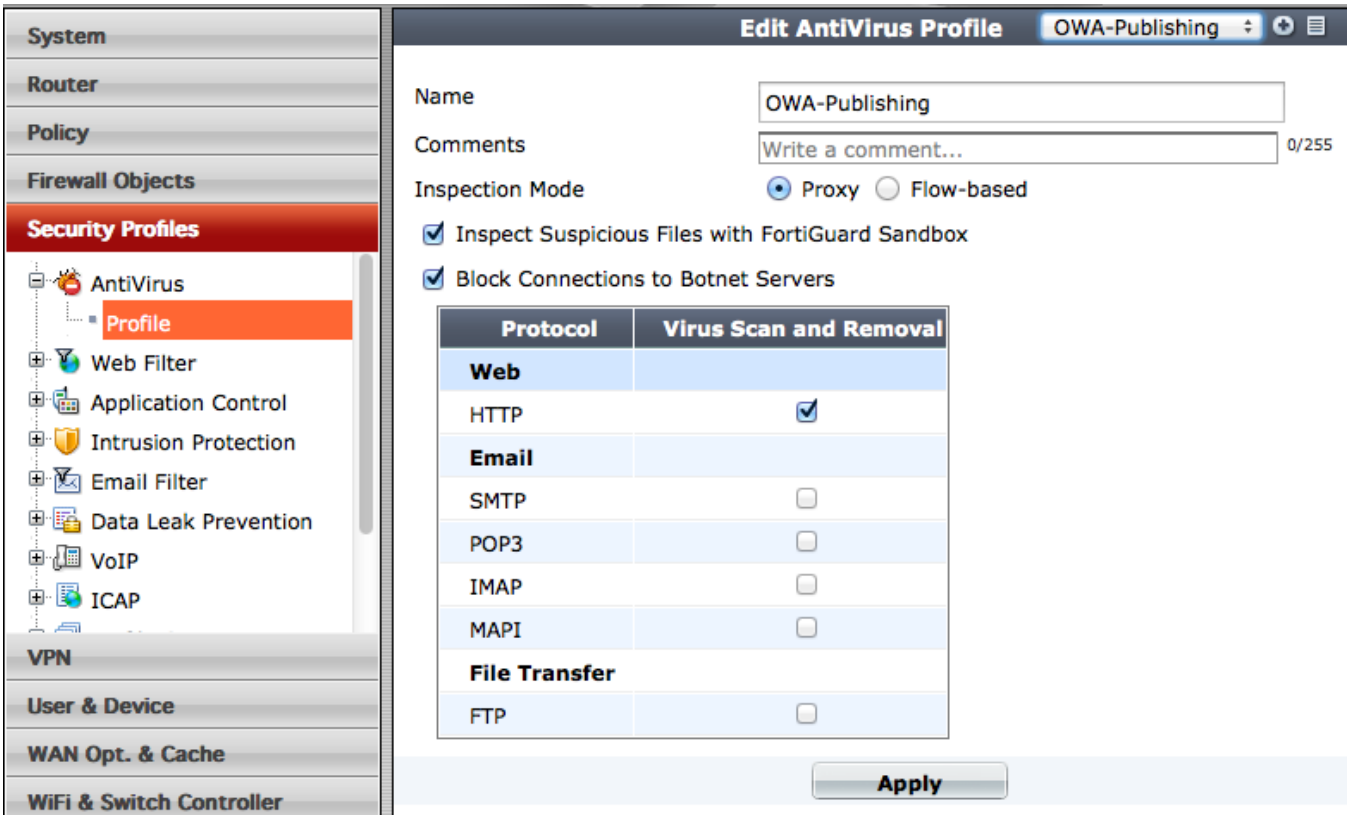
Another option is to check for failed authentication attempts. This can be enforced with a custom IPS signature. This following sample has been created to detect failed logins for OWA 2012:

```
config ips custom
edit "MS.OWA.Login.Error"
        set comment ''
        set signature "F-SBID( --attack_id 3608; --name
\"MS.OWA.Login.Error\"; --protocol tcp; --service http; --flow
from_server,reversed; --pattern \"<div class=|22|signInError|22
20|role=|22|alert|22|>\"; --context body; --no_case; --pattern
!\"<|2F|div>\"; --context body; --no_case; --within_abs 20; --rate
3,180;)"
    next
end
```

This signature will enable you to block the IP address of the client with 3 failed attempts within 180 seconds. These behavior can be changed with the “--rate 3,180;” parameters.

AntiMalware

The AntiMalware / AntiVirus feature is rather simple to configure.
Create a new Profile. Select Security Profiles / AntiVirus / Profile and click the plus sign ( )



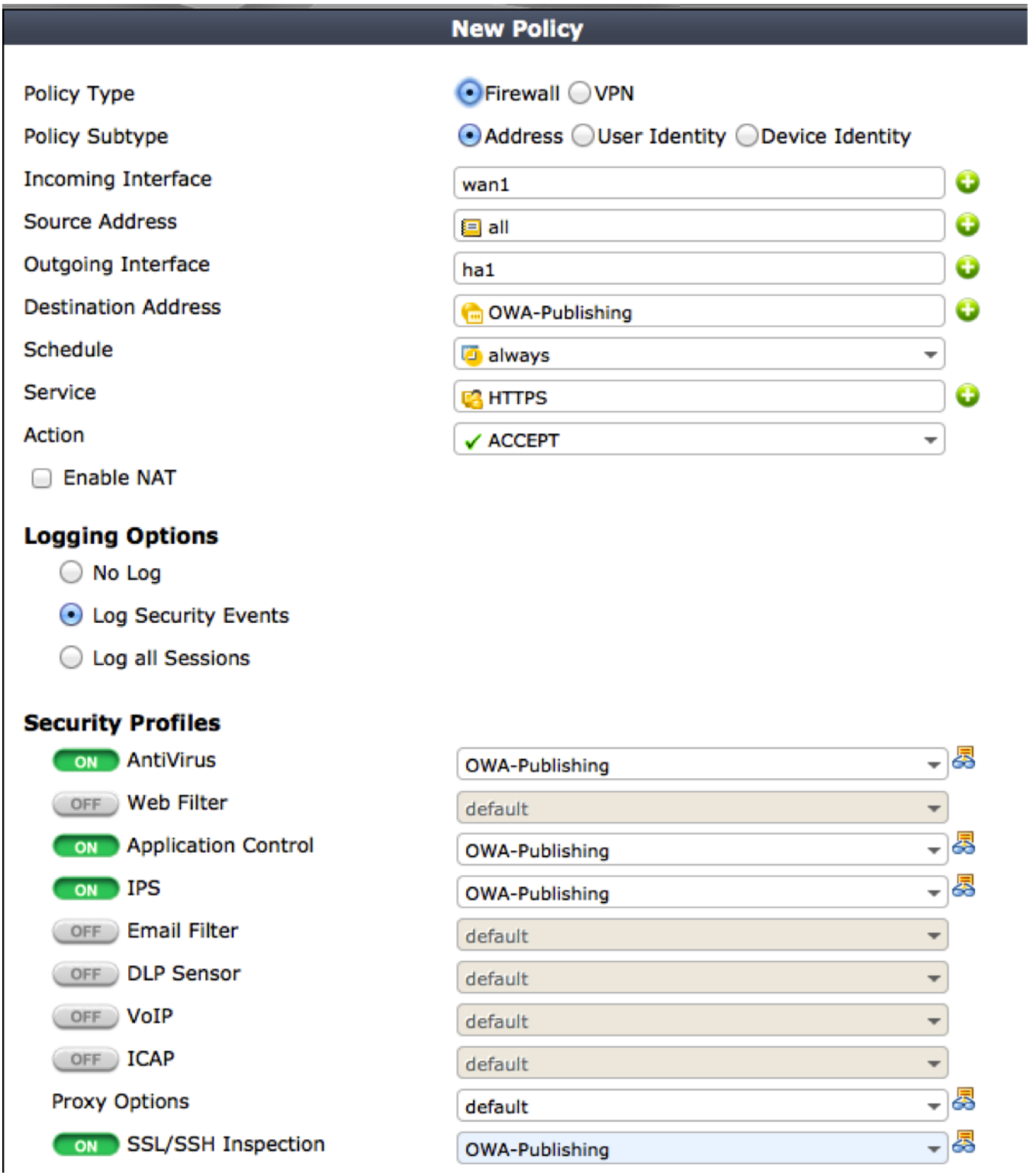
You can choose to submit suspicious files to the FortiGuard Sandbox and if you want to block connections from Botnet servers.
As the traffic for this application is purely HTTP(S), you can disable all other protocols in this profile.

URL Filter

As the Application Signature for OWA and Sharepoint verifies the URLs used by the client amongst others to identify the application, there is no immediate need to implement URL Filtering.

Putting it all together

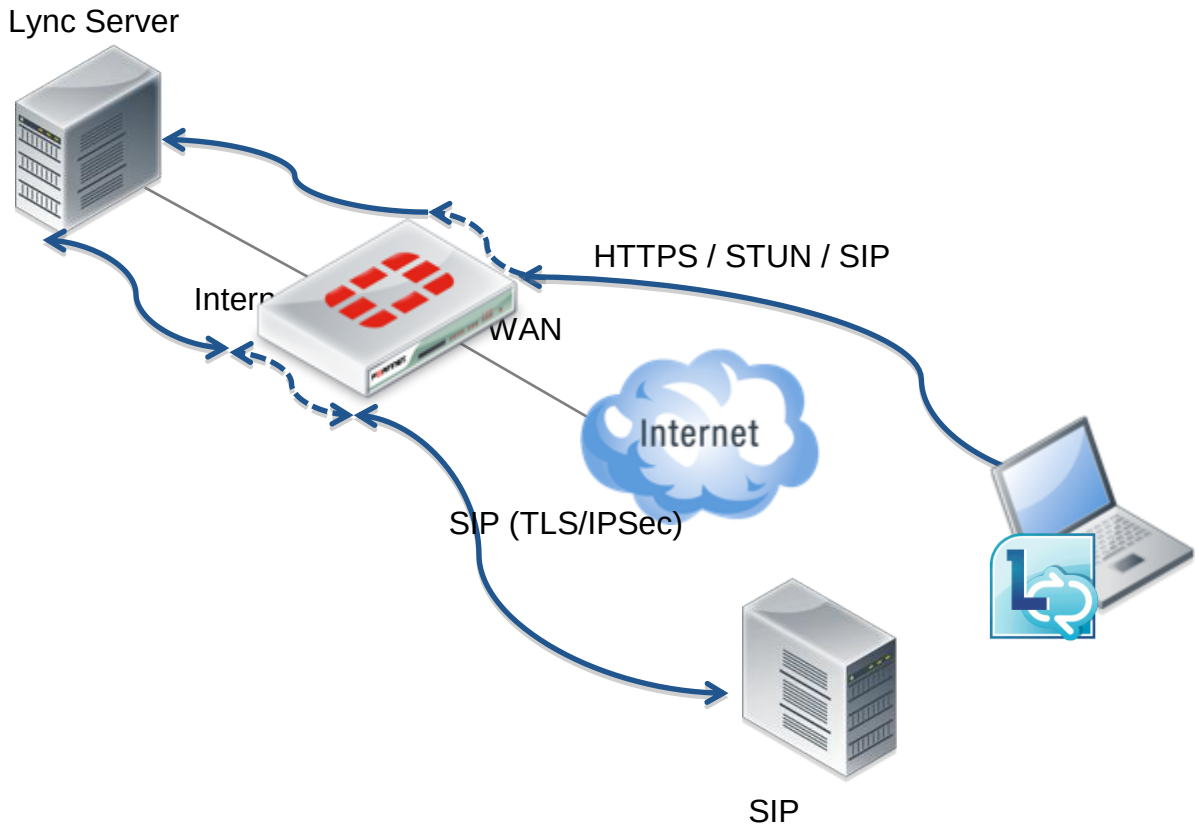
All you have to do now is enabling all the configured content security in the firewall policy that you already created.



Feature description

c. Lync Publishing

When publishing Lync services there are more communications protocols in use compared to OWA/SharePoint. But regarding infrastructure services the requirements stay the same. Again, public IP addresses need to be translated and SSL certificates changed accordingly on the perimeter side.



From a security standpoint the requirements increase due to additional communications protocols involved. The perimeter firewall needs to be able to check all these protocols.

The outcome of this is the following feature list:

- Scanning for attacks (Intrusion Prevention System)
- Scanning for viruses
- Checking of used paths for HTTP applications
- Checking on communications protocol in use (is it HTTP(S) or Activesync traffic/packets?)
- Layer 7 analysis of VoIP data
- Blocking of IP address and/or alarm administrators when there are failed login attempts
- Load sharing when using multiple application servers

Within FortiGate feature set, a SIP (TLS) application level gateway (ALG) has been implemented which enables detailed inspection and filtering of SIP traffic.

Implementing it

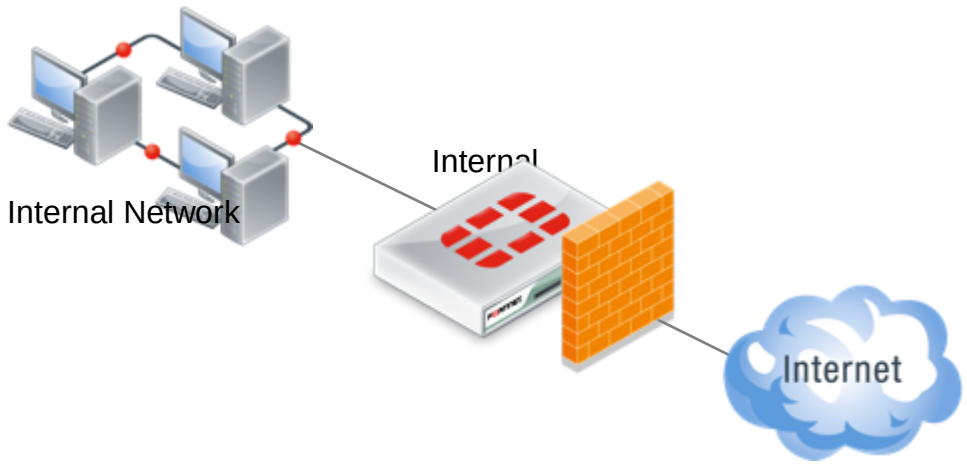
Lync consists of two communication paths, one for the HTTPS part and one for the SIP part of the communication.
The HTTPS communication can be configured similarly to the OWA/Sharepoint configuration.
The SIP configuration will be documented in a separate document.

d. Firewalling with Fortinet FortiGate

Feature Description

An UTM / Next Generation Firewall is the first line of defence against attacks from the Internet, protecting internal resources. At the same time unwanted communications from the inside to the outside has to be prevented.

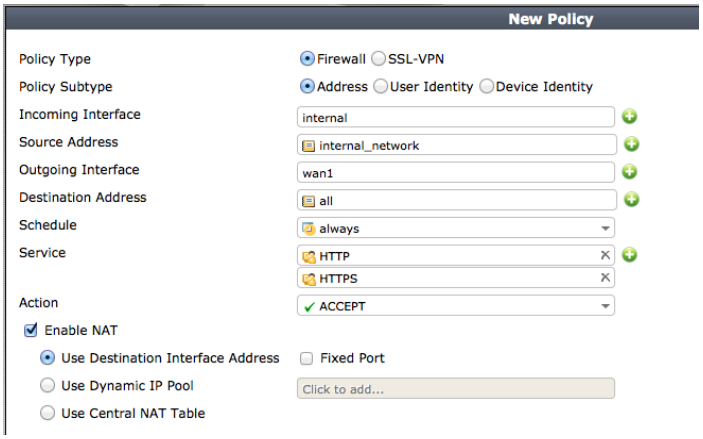
Core of all FortiGate models is the hardened operating system FortiOS which serves as a platform for multiple fully integrated security functions. That allows for defending against even advanced attacks and latest threats. Policies control flow of all data that traverses a FortiGate appliance. Statefull-Inspection firewall supplemented by security components such as AntiVirus, IPS, Application Control, Webfilter, etc. ensures secure communication. Multiple industry certifications prove the quality of FortiGate appliances. The ability to build identity based (on user or group information) firewall policies predestines FortiGate for homogenous Microsoft infrastructure environments with central user authentication and Single-Sign-On.



Implementing it

Classical firewalling was one of the initial features that FortiGate offered over 10 years ago.

Here is an example of a very simple firewall policy allowing everybody from the internal network to access HTTP and HTTPS on the Internet.



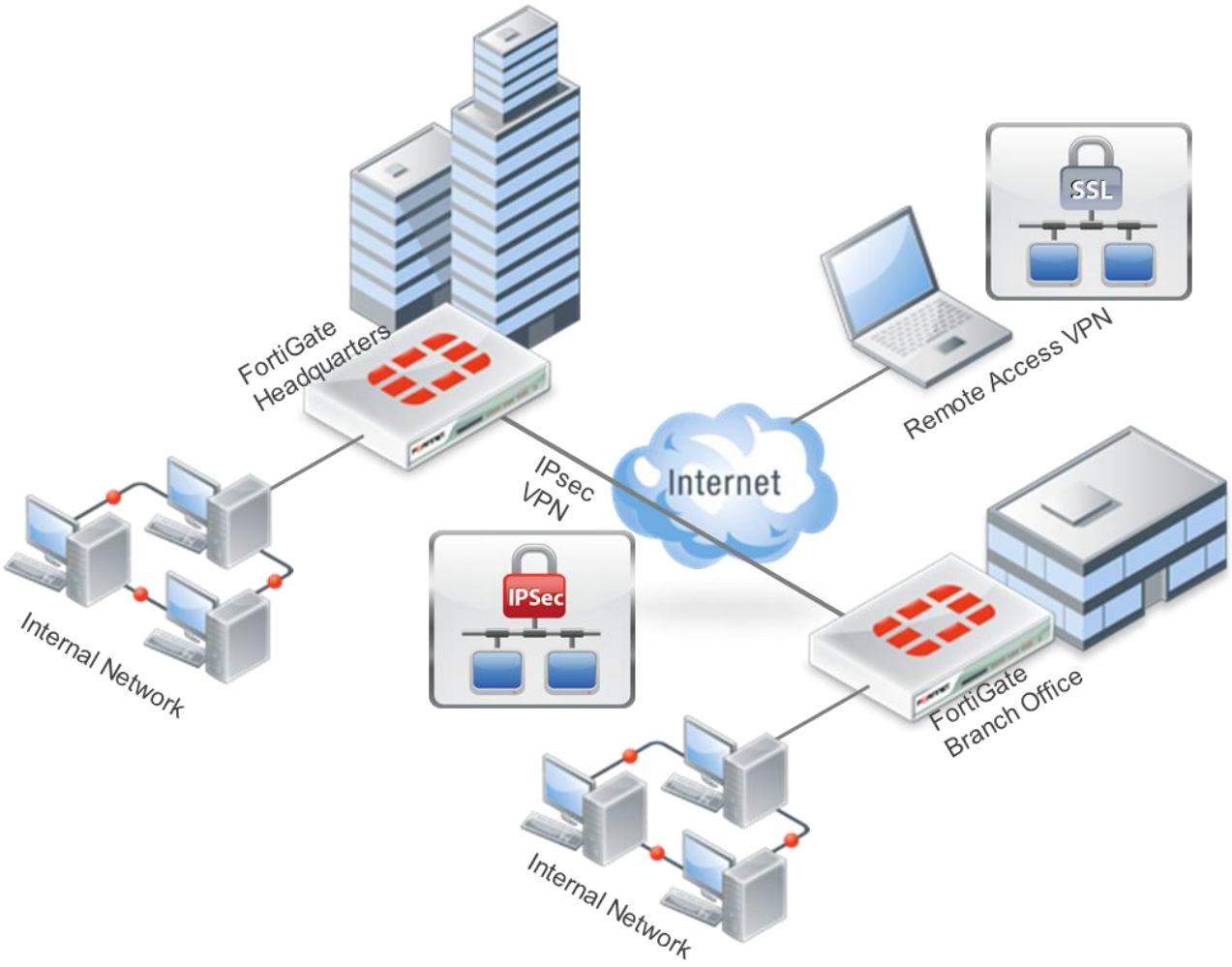
The firewall features are described in the FortiOS Handbook available on http://docs.fortinet.com

a. Virtual Private Networks with Fortinet FortiGate

Feature Description

Virtual Private Networks (VPN) allow secure, encrypted communication with company networks and resources. E.g. users may work from home or abroad and establish a secure connection from their smartphone or notebook using SSL VPN. The interconnect of various office locations can be achieved using persistent IPSec VPN tunnels.

Fortinet's FortiGate offers both remote access for mobile workers using SSL-VPN or



L2TP/IPSec and IPsec VPN for typical site-2-site communications between multiple locations. Beside pre-shared keys certificates are supported as well for authenticating devices and users. FortiToken is a one-time password solution directly built into the FortiGate operating system. If required it allows two factor authentication to securely authenticate mobile users.

Implementing it

FortiGate supports different kind of VPNs with different technologies.

Site2Site VPN

S2S VPN is typically used to connect 2 networks. FortiGate uses IPSec standard to achieve this. The Site2Site configuration is a standard implementation and is pretty good documented. There is nothing special in replacing a TMG installation here.

Please find related documentation here:
Documentation Page: http://docs.fortinet.com
Best practice examples: http://docs.fortinet.com/cookbook.html
Video tutorials: http://video.fortinet.com
Knowledgebase: http://kb.fortinet.com

Microsoft Windows Azure VPN

Microsofts Azure cloudservice uses IPSec Service as well. From a firewall point of view this is a Site2Site VPN configuration as well. Microsoft lists several vendors on their website and gives sample configuration scripts how to configure them.

Following you will find a configuration script in the same format as Microsoft publishes others for FortiOS 5

```
config vpn ipsec phase1-interface
    edit "Azure"
        set interface <NameOfYourOutsideInterface>
        set dhgrp 2
        set proposal aes256-sha1
        set dpd disable
        set remote-gw <SP_AzureGatewayIpAddress>
        set psksecret <SP_PresharedKey>
    next
end
config vpn ipsec phase2-interface
    edit "Azure-net1"
        set keylife-type both
        set pfs disable
        set phase1name "Azure"
        set proposal aes256-sha1 aes128-sha1
        set dst-subnet <SP_AzureNetworkCIDR>
        set keylifeseconds 3600
        set src-subnet <SP_OnPremiseNetworkCIDR>
    next
end
config router static
    edit 0
        set device "Azure"
        set dst <SP_AzureNetworkCIDR>
    next
```

```
end
config firewall address
    edit "OnPremiseNetwork"
        set subnet <SP_OnPremiseNetworkCIDR>
    next
    edit "AzureNetwork"
        set subnet <SP_AzureNetworkCIDR>
    next
end

config firewall policy
    edit 0
        set srcintf <NameOfYourInsideInterface>
        set dstintf "Azure"
        set srcaddr OnPremiseNetwork
        set dstaddr AzureNetwork
        set action accept
        set schedule "always"
        set service "ALL"
    next
end
```

Client VPN

FortiGate running FortiOS 5 supports the following techniques to secure communication with remote clients.

- IPSec
- SSL VPN
- L2TP
- PPTP

The clients can be authenticated using their Active Directory Credentials using LDAP to query the domain controller.

Additionally, FortiGate can send an e-mail or SMS to the user trying to create a VPN connection with a one-time password, that the user needs to enter before the authentication can be finished successfully.

According to Fortinets flat license philosophy this can be enabled without additional cost. Please not that sending an SMS requires an SMS gateway, which can create additional costs from your SMS provider.

Another alternative for two-factor authentication is FortiToken, a traditional 2 factor authentication key ring pendant. At the time of writing also available as an App for iPhone an Android

All methods are documented in the various sources:
Documentation Page: http://docs.fortinet.com
Best practice examples: http://docs.fortinet.com/cookbook.html
Video tutorials: http://video.fortinet.com
Knowledgebase: http://kb.fortinet.com

4. Fortinet products / Products - Featurematrix

Fortinet's broad range of FortiGate models offers a very flexible and effective tool to protect company networks. Due to the diversity of the different models the solution scales both technically and commercially from smallest offices (1-5 users) to enterprise environments (10.000 users and more).

An overview of all current FortiGate models can be found on the Fortinet Homepage at
http://www.fortinet.com/products/fortigate/

Depending on the TMG features and throughput required the following products could be taken into consideration when replacing TMG:

Modell	Firewall	VPN	Client-Proxy	OWA/SPS Publishing	Lync Publishing
FortiGate-90D And below	Yes	Yes	Yes	No	No
FortiGate-100D And above	Yes	Yes	Yes	Yes	Yes
FortiWeb all models	No	No	No	Yes[2]	Yes[3]

	Firewall (1518/512/64 byte)	Concurrent Sessions	New Sessions/Sec	IPSec VPN	IPS (HTTP)	Antivirus (Proxy/Flow)
FortiGate-60D	1.5 /1.5 /1.5 Gbps	500K	3.200	1 Gbps	200 Mbps	35 /50 Mbps
FortiGate-100D	2500 / 1000 / 200 Mbps	2.5 Mil	22.000	450 Mbps	950 Mbps	300/700 Mbps

A complete list of performance numbers is available on Fortinet's Website
http://www.fortinet.com/sites/default/files/basicfiles/ProductMatrix.pdf

[2] Including Single Sign On over multiple Sharepoint portals
[3] For HTTP(S) part of the connection, no SIP support